Integrating Cyber Losses into the Standard Microeconomics of the Consumer and Firm: Defining Losses in the Gordon and Loeb Model

Scott Farrow[1]
UMBC/CREATE

Integrating Information Sets into Micro-Economics

Gordon and Loeb (2002) obtained significant insight by abstracting cyber information sets from the remainder of the economic activity of the firm or organization. Information sets are interpreted broadly, potentially including data sets, websites, accounting information, algorithms, intellectual property, electronic communications, and so on. In their model and extensions (e.g. Farrow and Szanton, 2016) the effect of a cyber information breach results in a conditional loss, L, to the firm from any aspect of information security often considered to include confidentiality, integrity, authenticity, availability to users and non-repudiation. The loss is a part of an expected value objective function where probabilities are modeled separately. In Gordon, Loeb, Lucyshyn and Zhou (2015), the losses include external effects beyond the firm. There is however, value in re-integrating their sparsely defined conditional loss into the standard microeconomic modeling of the firm, the consumer, and government. Such reintegration will be shown to facilitate the decomposition of losses due to a breach, the differentiation of types of attacks on different parts of an organization, and the distinction between what GL refer to as private and external costs of an attack[2]

Microeconomics builds from an individual consumer and firm up to the market and general equilibrium levels. However, research on cyber losses to both consumers and firms has taken a more ad-hoc approach. Prior research seems to have taken two alternative approaches. One

[1] Appreciation is extended to Anupam Joshi, Matt Shabat and Jules Szanton. Funding was provided by the Department of Homeland Security National Center on the Risk and Economics of Terrorism Events.

[2] The economics of crime literature typically defines all attacks as types of externalities as there is no voluntary agreement to be attacked (Levinson, 2002 p. 337). Cyber security could be viewed as a subset of standard types of crime or terrorism that are enabled by computers and crimes or terrorism that are uniquely possible with computers (Anderson et al., 2012). The crime literature further debates whether the "thieves" have standing for costs and benefits with the usual but not universal conclusion that they do not. This is especially important for issues such as intellectual property or international cybercrime.

approach in the information technology literature is to develop taxonomies of types of attacks, potentially distinguished by their method of attack or the outcome (e.g. Undercofer, et al., 2003). A second approach has focused on cost categories. Detica (2011) focused on the costs associated with various stages of cyber-attacks, identifying categories of costs in anticipation, in consequence, in response, and indirect costs. Anderson, et al. (2012) organize their cost analysis using direct, indirect, and defensive costs with the cost to society being the sum of these categories.

In contrast to the existing work, the standard sequence of firm and consumer modeling is developed here in order to explicitly identify the several different pathways losses can occur. Such a delineation may encourage more detailed empirical modeling given the large research infrastructure built on analyzing common microeconomic structures. While the focus here is on the mechanism of losses due to some type of cyber activity, the dominant impact of cyber activity has been gains at least through all of the same mechanisms to be shown as capable of generating losses.

Cyber security and the consumer

Begin with the consumer who, for example, can be directly affected by breaches of Personal Identifying Information (PII) and whose choices creates the demand for a firm's product.

A deterministic model identifies goods Q_i that may have characteristics dependent on embedded cyber information and capabilities, **I** as is common with many consumer goods. Furthermore, transactions are facilitated by cyber information and processes typically embedded in computers, phones or other devices and linked to the internet. Consequently the good itself and its purchase is partially defined by cyber information, Q(**I**). Prices, P_i, are here assumed parametric in the budget constraint, Y such that:

$$\underset{Q_i}{\text{Max Utility}}\ (Q_1(\mathbf{I}), Q_2(\mathbf{I}), Q_3(\mathbf{I}) \ldots Q_n(\mathbf{I}))$$

$$\text{Subject to: } \sum_1^n P_i\,(\mathbf{I})\, Q_i\,(\mathbf{I}) = Y$$

The direct theft from a consumer, as perhaps from the loss of PII, can be modeled as a discrete decline in income[3], Y(**I**). More complexly, consider that characteristics of differentiated goods are identified both by their embedded use of cyber information through software, displays, controls and so on while the transaction cost and purchase context is also likely influenced by cyber information sets. To the extent that there are changes in the cyber information embedded in the good, prices[4], or income then the consumer's demand changes: $Q_i(\mathbf{I})=f(P_i(\mathbf{I}), P_j(\mathbf{I}), Y(\mathbf{I}), \mathbf{I})$.

The total derivative of the demand, focusing on is cyber components is thus:

$$dQ(\boldsymbol{I}) = \frac{\partial f}{\partial P_i}\frac{\partial P_i}{\partial \boldsymbol{I}}d\boldsymbol{I} + \frac{\partial f}{\partial P_j}\frac{\partial P_j}{\partial \boldsymbol{I}}d\boldsymbol{I} \ldots + \frac{\partial f}{\partial Y}\frac{\partial Y}{\partial \boldsymbol{I}}d\boldsymbol{I} + \frac{\partial Q}{\partial \boldsymbol{I}}d\boldsymbol{I}$$

The consumer's problem can also be written in terms of household production where household labor and purchased inputs yield household output (e.g. Becker, 1965; Gronau and Hammermesh, 2006). For instance, loss of an individual's time to re-establish identity or time involved with personal malware takes one to a household production model where time has a shadow price primarily measured by household labor. While not fully developing that model here, household labor, *H*, can be affected, both positively and negatively, by cyber information, hence *H*(**I**); as can household inputs such as electricity and water, HE(**I**) and HW(**I**) which are of concern due to potential cyber-physical infrastructure damage.

An information set (or just information) augmented consumer model thus captures: a) changes due to loss of income, b) costs associated with household production including unpaid time, c) changes in the quality of goods including the process of obtaining them, and c) potential changes in the utility function itself. For instance, the result of stolen PII from a retailer may involve changes in utility (and associated monetized value) reflected in a tighter budget constraint, having to spend time and other household inputs to restore their identity and changing their demand for products from that source or similar sources. In the latter case, there could be a

[3] As governments heavily depend on income taxes; such taxes could be modeled as depending on income and cyber information. For simplicity, such tax modeling is omitted here but included in the description of the firm.
[4] Note that to the extent effects are mediated through market price changes, then there can be usual "income" and substitution effects.

public bad of decreased quality across multiple goods, a topic investigated in more detail below. Alternatively, the primary effect of cyber information change can be positive for the consumer (as it typically has been from non-criminal use of cyber information). But even with a "loss" in by some other economic actor, as with intellectual property theft which may damage a particular firm's profitability, the existence of new competitors in a market may increase the welfare of consumers through the market mechanism.

Cyber security, the firm and government

Firms are linked to consumers via the demand (or inverse demand) function, shown above to depend on cyber information. But the firm's output also depends on its production function which is the maximum output from available inputs and based on a technology of production, f. Begin with a classical production function in which output, Q, is a function of capital and labor, f(K,L). Consideration is given first to the situation where no network or other externalities exist. The role of cyber information (or GL's information sets), I, can be modeled as both a stand-alone input and an intermediate input embedded in and affecting the productivity of K and L. The usefulness of considering the stand-alone portion occurs for instance, when considering theft of PII or intellectual property. The capital and labor within the firm would still operate with the same productivity, but a loss occurs. Examples of an effect mediated through capital and labor is malware which can affect the productivity of both inputs. Within a firm, initially augment a production function as Q(I)=f(L(I), K(I), I). Cyber security from the firm's perspective, absent externalities, is to consider how the production process is damaged if the *I* input is compromised, as from attacks which may affect confidentiality, integrity, authenticity, availability to users and so on. Further, *I* may affect the very definition of the output such that differentiated products may viewed by the consumer differently if they are secure or not, given some level of *I*.

Now consider the role of public goods (or bads) which is the mechanism through which externalities occur. Current production typically depends not only on the firm's own cyber information input, I, but also that of the external cyber system to which it is connected, **I,** comprised at least of all the linkages the firm uses on the internet or more indirect effects as through communications, control of utilities, and so on. Such a public good input may affect production directly or indirectly through other inputs. For instance, infrastructure damage to **I**

may both impair the firm's internal cyber information input as well as capital. Further, an attack over the internet may result in technological adaptation or response by the firm. While this could be considered an entirely new production function, here such responsive actions are modeled as direct shifts in output or shifts mediated through capital and labor with resulting implications for costs. A production function including both types of cyber information**,** internal and external, can then be written as $Q(I,\mathbf{I})=f(L(I, \mathbf{I}), K(I, \mathbf{I}), I(\mathbf{I}), \mathbf{I})$. Further, there is standard associated cost function representing the minimum cost of producing a level of output given the production function and input prices here shortened to focus on the role of information as $C(I, \mathbf{I})$.

The final element affected by cyber information is demand for the firm's product which, in perfect competition, is pre-determined at the firm level but jointly determined by supply and demand at the market level. At the market level, the internal cyber information is presumably so small as to not affect the price, but an external impact of cyber information may exist at the market level. Hence a competitive market price depends on external cyber information $P(\mathbf{I})$. For an imperfectly competitive firm, the price is normally a function of the firm's marginal revenue and marginal cost and, given the prominent role of internet sales and communication, also characterized as both a function of the internal and external cyber information, $P(I, \mathbf{I})$.

Consequently the pre-tax profit function for a firm can be written as $\pi(I, \mathbf{I})) = P(I,\mathbf{I})Q(I,\mathbf{I}) - C(Q(I,\mathbf{I}))$ with some the internal cyber information possibly irrelevant to a competitive firm. However, government and industry also interact in a variety of ways. The production function itself may be constrained by various regulatory policies with changes in policies resulting in a changed production function perhaps but not necessarily related to cyber information. More directly, a number of taxes transfer money from industry (and the consumer) to Government. The bi-directional impact of cyber information on taxes and tax revenue is here modeled by a tax on profits, $\tau(\pi(I,\mathbf{I}))$, although the focus below will be on the effect of the external effects. Including the tax effect allows for losses in government revenue potentially due to loss of intellectual property, or gains if government imposes taxes or fines on a firm due to cyber information breaches and or other actions.

Define the total potential private loss as the total derivative of the profit function:

$$d\pi(\mathrm{I},\mathbf{I}) \quad = \quad \frac{\partial \pi}{\partial \mathrm{I}} d\mathrm{I} + \frac{\partial \pi}{\partial \mathbf{I}} d\mathbf{I}$$

$$= \left[\frac{\partial P}{\partial \mathrm{I}} \, Q + P \frac{\partial Q}{\partial \mathrm{I}} - \frac{\partial C}{\partial Q} \frac{\partial Q}{\partial \mathrm{I}} dI - \tau \frac{\partial \pi}{\partial \mathrm{I}} \mathrm{dI} \right] + \left[\frac{\partial P}{\partial \mathbf{I}} \, Q + P \frac{\partial Q}{\partial \mathbf{I}} - \frac{\partial C}{\partial Q} \frac{\partial Q}{\partial \mathbf{I}} d\mathbf{I} - \tau \frac{\partial \pi}{\partial \mathbf{I}} \mathrm{d}\mathbf{I} \right]$$

One may also ask, what about financial dimensions of firms such as stock market prices, net worth, and borrowing costs? These financial dimensions are here considered derivative of the profit position of the firm. If profit expectations decline due to cyber breaches, that decline is expected to effect the financial condition of the firm including its net worth and such links could be followed analyzed through the impact on the profit function (e.g. Campbell et al., 2003).

Finally, Government is potentially affected by cyber information both through its own production and through its tax financing related to the production of firms and consumers. Regarding government production, the same pathways occur as with private firms with the caveat that neither costs are assumed to be minimized nor is social profit maximized. Hence government output is affected by both its internal and external cyber information, G(I,**I**) through the processes similar to those above.

Defining deterministic Losses

The literature on cyber costs uses various loss categories such as direct, indirect, defensive and so on. Such categories may be informative for particular data sets but are not economically well defined terms. Table 1 presents several candidate classifications based on widely used language from accounting, microeconomics and macroeconomics.

The distinction between the accounting terms "direct" and "indirect" has little classification power as cyber information losses (or gains) is spread across both production and "back office" processes which is central to the accounting definition. The distinction between private, external, and pecuniary effects from microeconomics has some classification power, although cyber losses are almost always initiated through an externality; they are not the result of a voluntary exchange. Like the spread of disease however, there can be an initial loss which is

spread as an additional externality, as through malware. Pecuniary externalities can exist as markets are affected. Finally, macroeconomic terms have some classification power by incorporating the production and market linkages across industries. For instance, the banking sector may incur losses from re-issuing cards as the result of a PII data breach in another industry. In short, the macroeconomics reminds us of industry interactions such as $\frac{\partial Qi}{\partial Qj}\frac{\partial Qj}{\partial \mathbf{I}}$ which may operate through the price mechanism, the legal system or other mechanisms. Similarly, interactions may occur through the endogeneity of the household sector as with induced effects. Finally, there may be political economic effects through government, including regulation.

Table 1: Loss categories from different professional framings

Term	Meaning
Accounting: direct and indirect	Direct associated with production or identifiable cost sector, compared with widely spread indirect costs
Microeconomics: private and external	Private: the result of voluntary exchanges while external effects are involuntarily incurred (positively or negatively) by third parties. Pecuniary externalities are third party effects mediated through market prices.
Macroeconomics: direct, indirect, induced	Whether at the industry level or firm level, direct output effects are identified with a change in output of a specific firm or industry while indirect effects are those from industry production or market linkages. Induced effects occur when households are endogenous to the system and expand or contract activity as part of a general equilibrium system. Secondary effects can be either or both of indirect or induced.

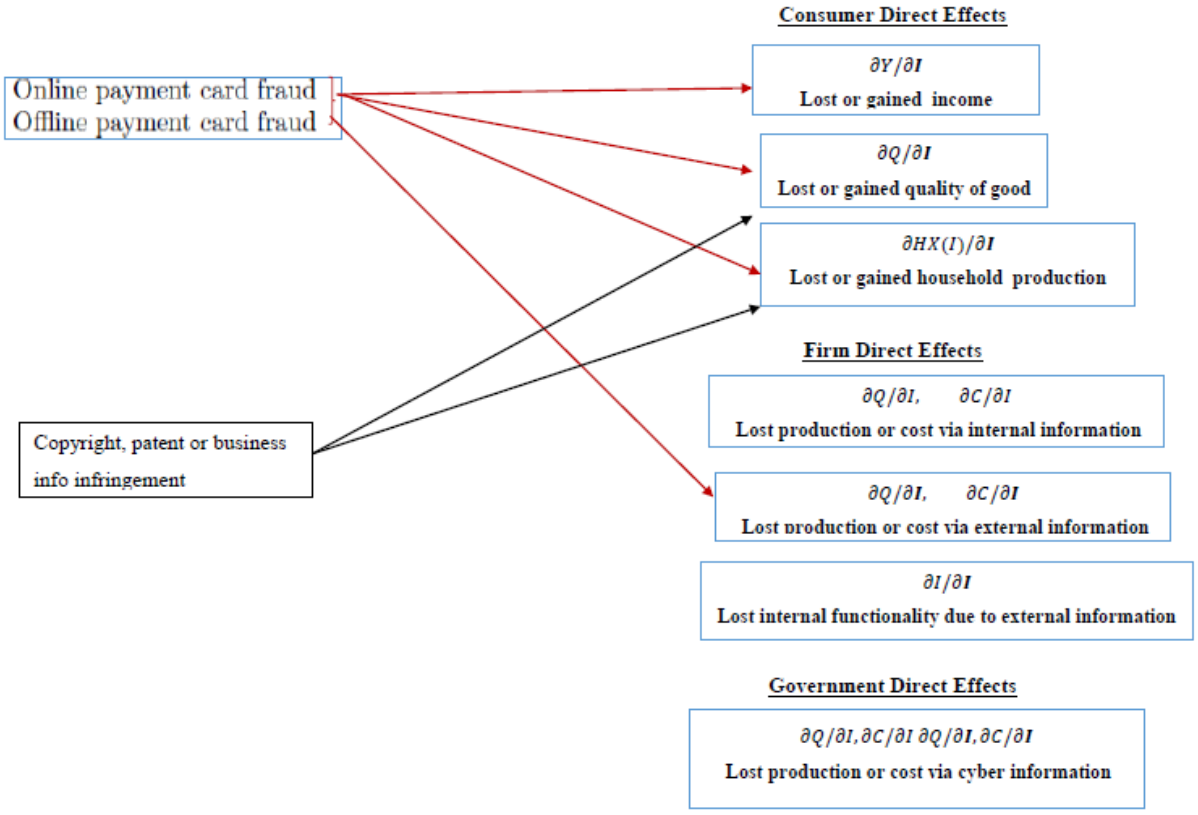
Consequently, direct effects are here taken to be the partial derivatives in the consumer, firm, and government problems that are not mediated through market prices or non-market responses such as regulation. Secondary (or indirect including induced) effects are those responses mediated through the market. The direct effects identified above are then the partial derivatives: $\partial Y/\partial \mathbf{I}, \partial Q/\partial \mathbf{I}, \partial HL(\mathbf{I})/\partial \mathbf{I}, \partial HX(\mathbf{I})/\partial \mathbf{I}$ for the consumer and $\partial Q/\partial$I, $\partial C/\partial$I ∂I$/\partial \mathbf{I}, \partial Q/\partial \mathbf{I}$, $\partial C/\partial \mathbf{I}$] for the firm, noting that $\partial \pi/\partial \mathbf{I}$ (associated with taxation) is affected by both direct and

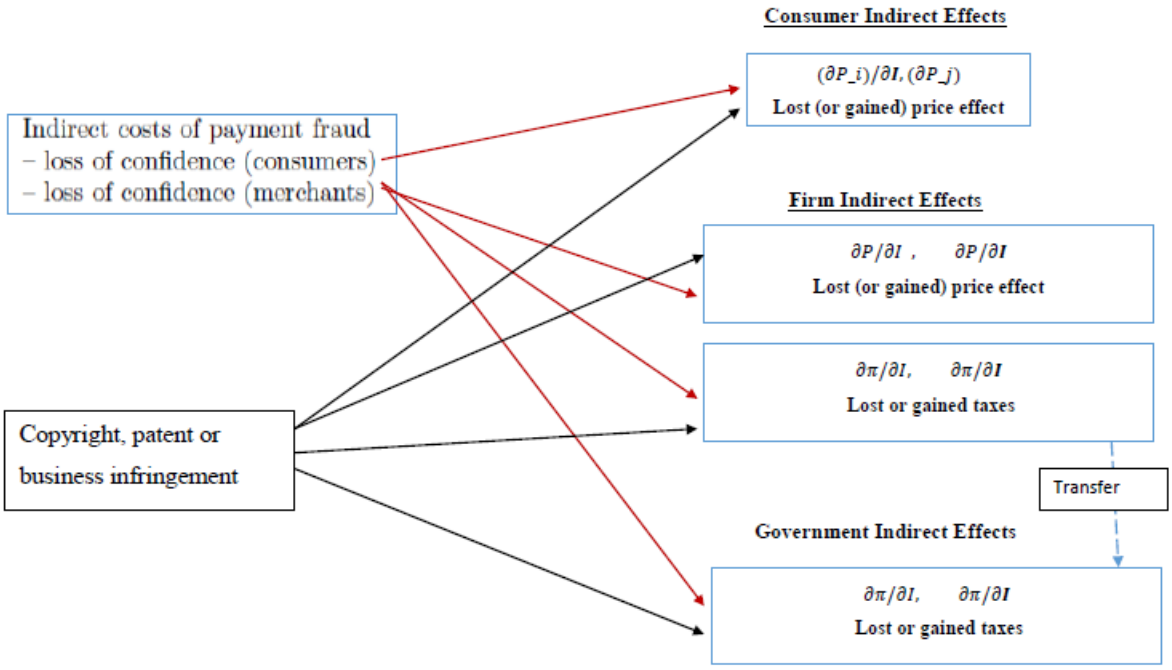
indirect changes to be further defined below. These direct effects are identified by the economic actor and the mechanism of impact rather than whether the actor chooses, for instance, to alter their production function via changes in software, capital, labor or some other aspect. Consequently, in the case of PII, both damages incurred by a consumer and monitoring or re-issue costs in the financial sector would be deemed direct, while possible changes in interest rates charged would be indirect as that latter is mediated through the market mechanism.

The secondary or indirect effects are then $\frac{\partial P_i}{\partial \mathrm{I}}, \frac{\partial P_j}{\partial \mathrm{I}}, \frac{\partial P_i}{\partial \mathbf{I}}, \frac{\partial P_j}{\partial \mathbf{I}}, \frac{\partial G}{\partial \mathrm{I}}, \frac{\partial G}{\partial \mathbf{I}}$ reflecting the interactions through the marketplace or regulation.

Illustrative components of Loss are presented in Figure 1. In addition to summarizing the categories of impact defined above, linkages are presented for two cost categories presented in Anderson, et al., (2012) to illustrate the partial mapping between the concepts.

Figure 1: Micro-economic categories of Loss for the consumer, firm and government separated into direct and indirect effects





This enumeration of core pathways for cost in standard economic terms has the potential to identify costs typically ignored, such as potentially positive or negative price effects, and to provide a structure in which to identify other pathways and elements of loss which may be omitted from the proposed structure. Economists are familiar with estimating elements of consumer demand and firm costs and production. The proposed framing of losses into a standard economic framework may facilitate the transition of empirical methodologies to cyber loss estimation.

Some Effects of Uncertainty and Conclusion

The loss estimates in GL and GLLZ are part of the objective function where the expected net benefits of cyber investments is maximized. The losses, elaborated upon above, are the

conditional losses where cyber security investment expenditures affect the probability of a successful attack. Continuing to focus on losses, the model of the consumer and firm has long been extended to conditions with uncertainty based on the expected utility model and more recently, non-expected utility models.

A natural extension to expected value optimization is expected utility maximization. To the extent that losses are potentially large so that a significant gamble is involved, then some risk aversion may be present (e.g. Eeckhoudt, Gollier and Schlesinger, 2005). Numerous methods exist in economics and decision analysis to elicit utility functions subject however, to the more restrictive assumptions that imply cardinal instead of ordinal utility (e.g. Clemen and Reilley, 2001; Keeney and Raiffa, 1976). The concern by some firms for a reputational effect from a cyber breach or intellectual property central to the firm or government may well warrant extending the model of losses to expected utility. Consideration of risk aversion leads naturally to consideration of insurance as a risk management strategy in addition to prevention.

However, the descriptive validity of the expected utility model is being questioned by behavioral economists and psychologists (DellaVigna, 2009) with a rich and rapidly evolving literature on consumer and firm behavior under uncertainty. That literature identifies a number of outcome anomalies such as the importance of reference points and asymmetric treatment of gains and losses as well as more complex treatment of probability than in the expected utility model. An analyst seeking a descriptive model of cyber losses may wish to include consideration of such factors. In empirical practice, such consideration can simply involve a different specification of an assumed utility function (Farrow and Scott, 2013).

Although this note has focused on defining conditional losses, two comments are made in regard to probability as cyber security investments were modeled as affecting the probability of the conditional loss. Given that framework, the dynamic aspect of cyber security—namely that new weakness are constantly being found and defenses are evolving over time—may best be incorporated into the probability function rather than making production functions dynamic although the latter remains a possibility. Similarly, behavioral models of probability as with cumulative prospect theory (Waaker, 2010) may be descriptively appropriate to consider.

In conclusion, identifying standard microeconomic structures helps identify the many pathways through which cyber losses can occur. Such identification may facilitate the use of econometric and other empirical methods commonly used with these structures.

References

Anderson, R., C. Barton, R. Boehme, R. Clayton, M. van Eeten, M. Levi, T. Moore, and S. Savage, 2012. Measuring the Cost of Cyber Crime, Workshop in the Economics of Information Security (WEIS).

Becker, Gary, 1965. A Theory of the Allocation of Time, *Economic Journal*, 75(Sept):493–517.

Clemen, R.T. and Reilley, T., 2001. *Making Hard Decisions*. Belmont CA: Duxbury Press (2001).

DellaVigna, Stefano, 2009. Psychology and Economics: Evidence from the Field. *Journal of Economic Literature*, 47:2, 315–372.

Gronau, R. and D. Hammermesh, 2006. Time vs. Goods: The Value of Measuring Household Production Technologies, Review of Income and Wealth, 52(1):1-16.

Gordon, L. and M. Loeb, 2002. The Economics of Information Security Investment, *ACM Transactions on Information and System Security*, 5(4):438-457.

Gordon, L., M. Loeb, W. Lucyshyn and L. Zhou, 2015. Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model, *Journal of Information Security*, 6:24-30.

Campbell, K., Gordon, L. A., Loeb, M. P., and Zhou, 2003. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431-448.

Cook P., and Graham, D., 1977. The Demand for Insurance and Protection: A Case of Irreplaceable Commodities. *Quarterly Journal of Economics*, 92:143-156.

Crawford, J., 2014. The U.S. government thinks China could take down the power grid, *CNN.com*, November 21, 2014. Available at <http://www.cnn.com/2014/11/20/politics/nsa-china-power-grid/>

Crosman, P., 2014. How Much Do Data Breaches Cost? Two Studies Attempt a Tally, *American Banker*, availiable at http://www.americanbanker.com/issues/179_176/how-much-do-data-breaches-cost-two-studies-attempt-a-tally-1069893-1.html

Detica and the Office of Cyber Security and Information Assurance. The cost of cyber crime, February 2011. https://www.gov.uk/government/publications/the-cost-of-cyber crime-joint-government-and-industry-report

Eeckhoudt, L., C. Gollier, and H. Schlesinger, 2005. *Economic and Financial Decisions Under Risk*, Princeton University Press, Princeton, NJ.

Farrow, S., 2007. The Economics of Homeland Security Expenditures: Foundational Expected Cost-Effectiveness Approaches, *Contemporary Economic Policy*, 25(1):14-26.

Farrow, S. and M. Scott, 2013. Comparing multi-state expected damages, option price and cumulative prospect measures for valuing flood protection, *Water Resources Research*, 49(5):2638-2648.

Farrow, S. and J. Szanton, 2016. Cybersecurity Investment Guidance: Extensions of the Gordon and Loeb Model, in press, *J. of Information Security*, February.

Friedman, Milton and Leonard Savage. 1948. The utility analysis of choices involving risk. *Journal of Political Economy*, 56(4):279-304.

Frankel, A., 2012. Can customers sue power companies for outages? Yes, but it's hard to win, *Reuters.com*, November 9, 2012. Available at <http://blogs.reuters.com/alison-frankel/2012/11/09/can-customers-sue-power-companies-for-outages-yes-but-its-hard-to-win/>

Graves, J., Acquiti, A., and Christin N., 2014. Should Payment Card Issuers Reissue Cards in Response to a Data Breach?, *WEIS: Workshop on the Economics of Information Security*, available at <http://www.econinfosec.org/archive/weis2014/papers/GravesAcquistiChristin-WEIS2014.pdf>

Hausken, K. 2006. Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability, *Information Systems Frontiers*, 8(5):338-349.

Herzog, S. 2011. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses, *Journal of Strategic Security*, 4, no. 2 (2011): 49-60. Available at <http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss>

Huang, C.D., Q. Hu and R. S. Behara, 2008. An economic analysis of the optimal information security investment in the case of a risk-averse firm, *International Journal of Production Economics*, 114:793– 804.

Kahneman, D., 2011. *Thinking Fast and Thinking Slow*, MacMillan.

Keeney, R. L., and H. Raiffa., 1976. Decision making with multiple objectives preferences and value tradeoffs. New York: Wiley.

Levinson, D., (ed)., 2002. *Encyclopedia of Crime and Punishment, Vol I.* Sage Publications.

Moore, T., R. Clayton and R. Anderson, 2011. The Economics of Online Crime. *Journal of Economic Perspectives*, 23(3):3-20.

Stewart, M, B. Ellingwood and J. Mueller, 2011. Homeland Security: A Case Study in Risk Aversion for Public Decision Making, *Int. J. Risk Assessment and Management,* 15(5/6): 367-386.

Stewart, M. and J. Mueller, 2013. Aviation Security, Risk Assessment, and Risk Aversion for Public Decisionmaking, *Journal of Policy Analysis and Management*, 32(3): 615–633.

Undercofer, J., A. Joshi and J. Pinkson, 2003. Modeling Computer Attacks: An Ontology for Intrusion Detection. Proceedings, Sixth International Symposium on Recent Advances in Intrusion Detection.

Wakker, P. (2010), *Prospect Theory for Risk and Ambiguity*, Cambridge University Press, Cambridge, UK.

Zhang, Z., 2013. *Cybersecurity Policy for the Electricity Sector: The First Step to Protecting Our Critical Infrastructure from Cyber Threats*, Boston University Journal of Science and Technology Law, Vol. 19 pp. 319-366.